# Erstellen von Cisco Secure Endpoint Linux Connector Kernel-Modulen

## Inhalt



# Einleitung

In diesem Artikel wird erklärt, wie man feststellt, wann vorkompilierte Kernelmodule, die für das Dateisystem des Cisco Secure Endpoint Linux Connectors und die Netzwerküberwachung erforderlich sind, für den derzeit laufenden System-Kernel nicht verfügbar sind, und wie Kernelmodule manuell kompiliert werden, damit die Dateisystem- und Netzwerküberwachung funktioniert.

Für die Zwecke dieses Artikels ist ein "nicht unterstützter Kernel" eine Kernel-Version, die vom Linux-Connector unterstützt wird, aber die speziellen vorkompilierten Kernel-Module, die für die Kernel-Version erforderlich sind, sind nicht im Connector-Installationspaket enthalten und müssen daher manuell kompiliert werden. Dies kann bei einer bestimmten Linux-Connector-Version der Fall sein, die auf einem Betriebssystem ausgeführt wird, das ein Roll Release-Update (z. B. Amazon Linux 2) verwendet.

Nicht alle Linux-Distributionen und Kernel-Versionen unterstützen kompilierte Kernel-Module. Dieser Artikel hilft bei der Identifizierung, wenn man Kernel-Module manuell kompilieren kann.

# Voraussetzungen

## Anforderungen

- Bei RHEL-basierten Systemen ist ein von der Distribution bereitgestellter gcc installiert. Kernel-devel installiert für derzeit laufenden Kernel.
- Bei Systemen, die einen Unbreakable Enterprise Kernel (UEK) verwenden, ist ein von der Distribution bereitgestellter gcc installiert. kernel-uek-devel installiert für derzeit laufenden Kernel.

# Geltungsbereich

## Betriebssystem

- RHEL/CentOS 7
- Oracle Linux 7 Red Hat Compatible Kernel (RHCK)
- Oracle Linux 7 UEK 5 oder frühere Version
- Amazon Linux 2

# Kernel-Versionen

- Das Netzwerk-Monitoring-Kernelmodul kann für Kernel-Versionen 2.6 bis 4.14 kompiliert werden.
- Das Kernel-Modul für die Dateisystemüberwachung kann für Kernel-Versionen 3.10 bis 4.14 kompiliert werden.

HINWEISE:

- Auf Kernel-Versionen 2.6 bis 3.10 verwendet der Connector redirfs (ein Out-of-Tree-Kernelmodul) für die Dateisystemüberwachung, die nicht für die benutzerdefinierte Kompilierung anwendbar ist.
- Kernel-Versionen zwischen 4.14 und 4.19 sind nicht mit dem Connector kompatibel und auch nicht für die benutzerdefinierte Kompilierung geeignet.
- Für Kernel-Versionen 4.19 und neuer verwendet der Connector eBPF-Module für die Dateisystem- und Netzwerküberwachung. Weitere Informationen zur Behebung dieses Fehlers für diese Kernel-Versionen finden Sie im Linux Kernel-Devel Fault-Artikel.

# Connector-Versionen

- 1.16.0 und höher
- 1.18.0 und höher zum Erstellen benutzerdefinierter UEK-Kernelmodule

## Diagnähen Ein nicht unterstützter Kernel

Wenn der Connector auf einem Computer mit einem nicht unterstützten Kernel ausgeführt wird, werden Fehler 8 (Realtime-Dateisystemmonitor konnte nicht gestartet werden) und Fehler 9 (Realtime-Netzwerkmonitor konnte nicht gestartet werden) ausgelöst, und der Connector wird in einem heruntergestuften Zustand ohne Dateisystem- oder Netzwerküberwachung ausgeführt.

Die folgenden Schritte können von einem Terminalfenster aus durchgeführt werden, um zu ermitteln, ob der Anschluss auf einem nicht unterstützten Kernel ausgeführt wird:

1. Stellen Sie sicher, dass Fehler 8 und/oder Fehler 9 ausgelöst wurde:

```
$ /opt/cisco/amp/bin/ampcli status [logger] Set minimum reported log level to notice Trying to connect... Connected. Status: Connected Mode: Degraded Scan: Ready for scan Last Scan: none Policy: unsupported kernel example (#7607) Command-line: Enabled Faults: 2 Critical Fault IDs: 8, 9 ID 8 - Critical: Realtime filesystem monitor failed to start. ID 9 - Critical: Realtime network monitor failed to start.
```

2. Stellen Sie sicher, dass der aktuelle Kernel inklusive zwischen 2.6 und 4.14 liegt und keiner der vorkompilierten Kernel-Modulversionen entspricht.
   Der folgende Befehl zeigt die aktuelle Kernel-Version an:

```
$ uname -r 4.14.97-90.72.amzn2.x86_64
```

Die verfügbaren vorkompilierten Kernel-Modulversionen, die mit dem Connector verpackt sind, werden mit dem folgenden Befehl aufgelistet:

3.

```
$ ls /opt/cisco/amp/bin/modules/ 4.14.186-146.268.amzn2.x86_64 4.14.198-
152.320.amzn2.x86_64 4.14.209-160.335.amzn2.x86_64 4.14.219-161.340.amzn2.x86_64 4.14.225-
169.362.amzn2.x86_64 4.14.192-147.314.amzn2.x86_64 4.14.200-155.322.amzn2.x86_64 4.14.209-
160.339.amzn2.x86_64 4.14.219-164.354.amzn2.x86_64 4.14.231-173.360.amzn2.x86_64 4.14.193-
149.317.amzn2.x86_64 4.14.203-156.332.amzn2.x86_64 4.14.214-160.339.amzn2.x86_64 4.14.225-
168.357.amzn2.x86_64 4.14.231-173.361.amzn2.x86_64
```

Im obigen Beispiel ist die Kernel-Version 4.14.97-90.72.amzn2.x86_64 nicht in der Liste der verfügbaren Kernelmodule enthalten.

Der Linux-Connector ist für das Kompilieren benutzerdefinierter Kernelmodule geeignet, wenn alle der folgenden Bedingungen zutreffen:

- Beim Anschluss werden Fehler 8 und/oder 9 ausgelöst.
- Die aktuelle Kernelversion liegt inklusive zwischen 2.6 und 4.14.
- Die aktuelle Kernel-Version ist nicht in der Liste der vorkompilierten Kernelmodule `/opt/cisco/amp/bin/modules` enthalten

# Auflösung

Wenn ein Linux-Connector auf einem nicht unterstützten Kernel ausgeführt wird, kann die folgende Prozedur verwendet werden, um benutzerdefinierte Kernelmodule für das System zu kompilieren:

1. Erforderliche Systemabhängigkeiten installieren:

```
$ yum install gcc
```

`gcc` ist erforderlich, um die Kernelmodule mit spezifischen Optionen zu kompilieren.Auf Systemen, die einen RHEL-basierten Kernel verwenden, verwenden Sie den folgenden Befehl, um das erforderliche Kernel-Paket zu installieren:

```
$ yum install kernel-devel-$(uname -r)
```

Auf Systemen, die UEK verwenden, verwenden Sie den folgenden Befehl, um das erforderliche Kernel-Paket zu installieren:

```
$ yum install kernel-uek-devel-$(uname -r)
```

Abhängig von Ihrem System ist `kernel-devel-$(uname -r) orkernel-uek-devel-$(uname -r)` erforderlich, um die Kernelmodule für den aktuellen Kernel zu kompilieren.

2. Führen Sie das Skript compile_kmods.sh mit Root-Berechtigungen aus:

```
$ sudo /opt/cisco/amp/bin/compile_kmods.sh
```

Das compile_kmods.sh-Skript versucht, Dateisystem- und Netzwerküberwachungs-Kernelmodule für die aktuelle Kernel-Version zu kompilieren. Die benutzerdefinierten Kernel-Module werden unter dem `/opt/cisco/amp/extras/modules` Verzeichnis. Am Ende der Ausführung startet das Skript den Connector automatisch neu, sodass die neu kompilierten Kernelmodule auf das System geladen werden können.

3. Bestätigen Sie, dass die Fehler 8 und 9 behoben wurden:

```
$ /opt/cisco/amp/bin/ampcli status [logger] Set minimum reported log level to notice Trying
to connect... Connected. Status: Connected Mode: Normal Scan: Ready for scan Last Scan:
```

```
2021-06-14 05:53 PM Policy: unsupported kernel example (#7607) Command-line: Enabled
Faults: None
```

## Weitere Befehle

Die ausführbare Datei compile_kmods.sh ist in Secure Endpoint Linux Connector Versionen 1.16.0 und neuer verfügbar und wird automatisch auf kompatiblen Betriebssystemversionen installiert. Die ausführbare Datei compile_kmods.sh wurde in Secure Endpoint Linux Connector Version 1.18.0 und neuer verbessert, um die benutzerdefinierte Kompilierung von UEKs zu unterstützen.

Die benutzerdefinierte Kompilierung von Kernelmodulen für die Netzwerküberwachung wird auf Kernel-Versionen 2.6 bis 4.14 unterstützt, während die benutzerdefinierte Kompilierung von Kernelmodulen für die Dateisystemüberwachung auf Kernel-Versionen 3.10 bis 4.14 unterstützt wird.

### Verfügbare Befehle

**HINWEIS:** Die ausführbare Datei compile_kmods.sh muss mit Root-Berechtigungen ausgeführt werden.

- Die Option`-h/-help` zeigt eine vollständige Liste der verfügbaren Optionen an:

```
$ /opt/cisco/amp/bin/compile_kmods.sh --help Usage: compile_kmods [OPTIONS] OPTIONS: -f, --
force force overwriting compiled kmod -h, --help show help
```

- Die `-f/-force`-Option kann verwendet werden, um ein zuvor kompiliertes benutzerdefiniertes Kernelmodul zu erzwingen, damit der aktuell ausgeführte Kernel überschrieben wird. Dies sollte verwendet werden, wenn das aktuelle benutzerdefinierte Kernelmodul mit einer älteren Version des Connectors erstellt wurde und mit einer aktualisierten Version des Connectors kompiliert werden muss. Der Connector-Update-Prozess kompiliert die Kernel-Module des Kunden nicht im Rahmen des Updates neu.

# Fehlerbehebung

Wenn Fehler 8 und/oder 9 nach dem *Auflösung* Es werden die folgenden Schritte ausgeführt, um das Problem weiter zu untersuchen:

- Suchen Sie im Systemprotokoll`/var/log/messages nach Protokollzeilen`, die den folgenden entsprechen: Im folgenden Protokoll wird angegeben, dass die aktuelle Kernel-Version auf dem Computer keine Kernelmodule für die Dateisystem- und Netzwerküberwachung verwendet. Auf Kernel-Versionen größer oder gleich 4.18 werden das Dateisystem und das Netzwerk mithilfe von eBPF-Modulen überwacht.

```
init: cisco-amp pre-start: AMP kernel modules are not required on this kernel version
'5.4.117-58.216.amzn2.x86_64'; skipping reinstalling kernel modules
```

  Im folgenden Protokoll wird angegeben, dass im Verzeichnis der vorkompilierten Kernelmodule keine Kernelversionen gefunden wurden. `/opt/cisco/amp/bin/modules`, die mit der aktuellen Kernel-Version kompatibel sind:

```
init: cisco-amp pre-start: finding compatible kernel modules in /opt/cisco/amp/bin/modules
to install init: cisco-amp pre-start: failed to find kernel versions init: cisco-amp pre-
start: failed to install and load all required kernel modules in /opt/cisco/amp/bin/modules,
continuing without some modules loaded
```

Im folgenden Protokoll wird angegeben, dass im benutzerdefinierten Verzeichnis der kompilierten Kernelmodule keine Kernelversionen gefunden wurden. `/opt/cisco/amp/extra/modules`, die mit der aktuellen Kernel-Version kompatibel sind:

```
init: cisco-amp pre-start: finding compatible kernel modules in /opt/cisco/amp/extra/modules
to install init: cisco-amp pre-start: failed to find kernel versions init: cisco-amp pre-
start: failed to install and load all required kernel modules in
/opt/cisco/amp/extra/modules, continuing without some modules loaded
```

- Überprüfen Sie, ob Secure Endpoint Linux Connector-Dateisystem und Netzwerküberwachungs-Kernelmodule geladen werden:

```
$ lsmod | grep ampfsm ampfsm 24576 0
```

```
$ lsmod | grep ampnetworkflow ampnetworkflow 65536 0
```

- Führen Sie ein Upgrade des Secure Endpoint Linux-Connectors auf eine neuere Version durch, falls verfügbar.